

MATHÉMATIQUES

Géométrie et ordinateurs (II)

Sphères discrètes, réduction des bases de \mathbb{Z}^n

Jean-Pierre REVEILLÈS

(LLAIC1, Université d'Auvergne reveil@llaic.u-clermont1.fr)

1 – Introduction

La complexité des algorithmes rencontrés en mathématique discrète vient souvent de l'augmentation des dimensions ou de la taille des données à traiter, mais ce n'est pas la seule cause. Dans de nombreuses applications de nature plus géométrique (voir entre autres [4], [7], [10], [11], [15], [16], [17], [18]), elle est assez directement liée à des concepts algébriques et arithmétiques et assez souvent on voit surgir la fameuse *réduction des bases des sous-groupes de \mathbb{Z}^n* . Cette deuxième partie donne un tel exemple d'apparition de cette question dans l'étude des sphères discrètes.

De nombreux travaux et plusieurs algorithmes, dont le célèbre LLL ([13]), sont liés à la *réduction des bases*. L'étude de certains objets discrets définis par des solutions d'inéquations diophantienne simples et surtout l'algorithmique associée, nous obligent à revoir ce problème sous un angle plus géométrique. Nous pensons également que la didactique de ce type de sujet peut, en retour, profiter de cette approche plus géométrique. Après une présentation détaillée d'une approche géométrique de la réduction en dimension 2 nous donnons sa généralisation à l'aide des sphères circonscrites à des simplexes de dimension quelconque.

C'est volontairement que nous nous restreignons à la réduction des réseaux *discret*, (i.e. dans \mathbb{Z}^n), même si quelques concepts euclidiens classiques sont employés pour la commodité de l'exposé. Ce choix se justifie par les relations que la Géométrie Discrète entretient avec la Géométrie Algorithmique, la Cristallographie et de nombreux domaines de l'Informatique. On apprend beaucoup sur ces questions en les traitant algorithmiquement, c'est pour cette raison que quelques bouts de code très succints, écrits avec *Maple* sont joints à cette partie.

2 – Enveloppe convexe des sphères discrètes

Comme pour les cercles discrets introduits dans la première partie, la sphère discrète \mathcal{S}_R peut être considérée comme l'ensemble des *points frontière* de la boule discrète définie par l'inéquation $x^2 + y^2 + z^2 < (R + \frac{1}{2})^2$.

L'algorithme suivant construit la partie de la sphère discrète \mathcal{S}_R formée des points qui satisfont aussi aux inégalités $0 \leq x \leq y \leq z$; c'est, plus précisément, un 48-ième de la sphère complète; cette partie peut être considérée comme un domaine fondamental du groupe des symétries d'un cube. Sa projection sur le plan xOy est le quart d'ellipse $x^2 + 2y^2 < (R + \frac{1}{2})^2, x \geq 0, y \geq 0$.

La variable tmp_e permet de construire le bord de cette ellipse en suivant le point courant de coordonnées (x, y_e) de manière incrémentale; (l'affichage, qui n'est pas traité ici, peut être facilement réalisé avec le logiciel mentionné).

```

 $x = 0; y = 0; z = 0; tmp = R^2 + R$ 
 $y_e = [R\sqrt{(2)}/2]; tmp_e = tmp;$ 
pour  $x = 0$   $R$  faire
  pour  $y = 0$   $y_e$  faire
     $point(x, y, z);$ 
     $tmp = tmp + 2y + 1;$ 
     $y = y + 1;$ 
    si  $tmp \geq R^2 + R + 1$ 
      alors
         $tmp = tmp - 2z + 1; z = z - 1$ 
      fin si
    fin pour
   $tmp_e = tmp_e + 2x + 1$ 
  si  $tmp_e \geq R^2$ 
    alors
       $tmp_e = tmp_e - 4y_e + 2;$ 
       $y_e = y_e - 1$ 
    fin si
  fin pour

```

Soient $M = (x, y, z)$ un point de \mathcal{S}_R et $\nu = (\alpha, \beta, \gamma)$, $\nu' = (\alpha', \beta', \gamma')$ deux directions entières. Le produit vectoriel $\nu \wedge \nu'$ donne le vecteur normal à la face définie par M et les deux directions ν et ν' ; il est désigné par $n = (a, b, c)$. Cette fois notre problème nécessite l'étude des deux cercles d'intersection définis par les plans $aX + bY + cZ = k$ et $aX + bY + cZ = k + 1$, où $k = ax + by + cz$, avec la sphère euclidienne $X^2 + Y^2 + Z^2 = (R + \frac{1}{2})^2$. La partie essentielle du travail consiste à calculer la distance du point d'intersection I de la droite dirigée par $n = (a, b, c)$ et du plan $aX + bY + cZ = k + 1$, de coordonnées

$$I = (k + 1)(a^2 + b^2 + c^2)^{-1}(a, b, c),$$

au réseau entier défini par l'équation

$$aX + bY + cZ = k + 1.$$

Nous avons vu dans la première partie deux cas d'évaluation arithmétique de cette distance qui sera encore notée r comme précédemment; on a aussi le résultat suivant.

Théorème 1. — *La face définie par le point M et les deux vecteurs ν et ν' , est une face de l'enveloppe convexe de \mathcal{S}_R si et seulement si on a*

$$r^2 > \left(R + \frac{1}{2}\right)^2 - \frac{(ax + by + cz + 1)^2}{a^2 + b^2 + c^2}.$$

La généralisation du théorème 1 (de la partie I) aux sphères discrètes nécessite donc de savoir trouver le point d'un sous-groupe de rang 2, \mathcal{G} , de \mathbb{Z}^3 le plus proche d'un point (rationnel) donné du plan euclidien défini par \mathcal{G} . Ce problème suppose lui-même que l'on sache trouver la *base minimale* d'un groupe tel que \mathcal{G} . Ces questions sont traitées plus loin.

Dans notre cas le groupe \mathcal{G} est défini par une équation diophantienne :

$$ax + by + cz = 0,$$

il s'agit donc de déterminer la base minimale du sous-groupe \mathcal{G} de \mathbb{Z}^3 orthogonal à la direction entière (a, b, c) normale à la face testée.

3 – Algorithme de réduction d'une base d'un sous-groupe de \mathbb{Z}^2

On considère une base $\mathcal{B} = (OU, OV)$ d'un sous-groupe \mathcal{G} de \mathbb{Z}^2 . Il suffit de résoudre ce cas particulier pour savoir réduire une base d'un sous-groupe de rang 2 de \mathbb{Z}^n .

Soient $OU = (a, b), OV = (c, d)$ les composantes de ces vecteurs ; on suppose que le déterminant $\delta = ad - bc$ de \mathcal{B} est positif. Donnons un critère de minimalité commode pour une telle base ; celui-ci sera généralisé plus loin au §8.

En général le cercle circonscrit au triangle OUV d'une base \mathcal{B} contient beaucoup d'autres points de \mathcal{G} sauf si \mathcal{B} est *minimale* auquel cas il ne contient plus que les trois points O, U et V . Le cercle circonscrit à la base (OU, OV) de la figure 1 contient de nombreux points du sous-groupe \mathcal{G} dont les éléments sont représentés par de gros points. Par contre dans le cercle circonscrit au triangle OUV' seuls les trois sommets sont dans \mathcal{G} ; la base $\{OU, OV'\}$ est minimale.

Cette propriété de la base $\{OU, OV'\}$ est connue en géométrie algorithmique où l'on dit que OUV' est un *triangle de Delaunay* du réseau \mathcal{G} (cf. [1]). Les assertions précédentes se déduisent du théorème suivant.

Théorème 2. — *Soit \mathcal{G} un sous-groupe de \mathbb{Z}^2 et (OU, OV) l'une de ses bases. Les trois propriétés suivantes sont équivalentes :*

- a) *le centre du cercle circonscrit à OUV est intérieur au triangle OUV ,*
- b) *(OU, OV) est base minimale de \mathcal{G} .*
- c) *OUV est un triangle de Delaunay du réseau \mathcal{G} .*

Bien que la preuve de ces équivalences soit immédiate nous l'incluons dans le souci de rendre l'article le plus autonome possible. Si l'on désigne par $\Delta(OU)$ la bande parallèle du plan euclidien orthogonale au côté OU du triangle OUV délimitée par les extrémités O et U , on voit que l'algorithme de réduction consiste en particulier à déterminer le point V de la droite de Bézout associée à OU contenu dans $\Delta(OU)$. On dit dans ce cas que le côté OU vérifie la propriété (μ) . De la même manière l'algorithme conduit à modifier les sommets U et V de telle sorte que les deux côtés OU et OV vérifient la condition (μ) . Ceci

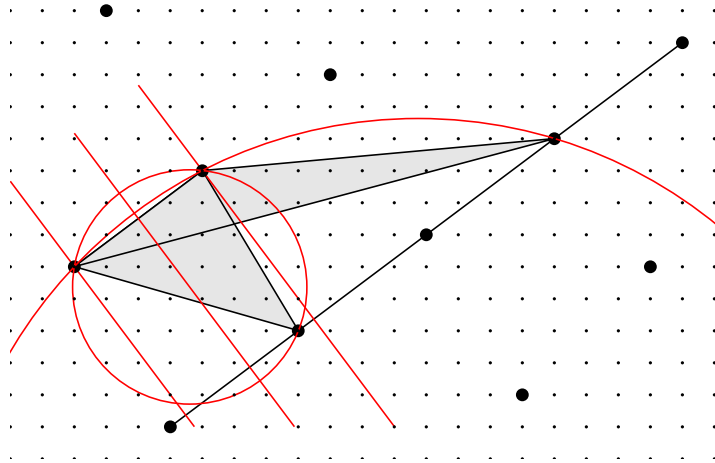


FIG. 1. *

Figure 1. — Réduction de la base d'un réseau

équivalent à dire que les médiatrices de OU et OV se coupent à l'intérieur du triangle OUV (et que le côté UV vérifie aussi la condition (μ)). Autrement dit l'assertion a) du théorème équivaut à dire que les 3 côtés du triangle OUV vérifient (μ) .

Montrons que a) entraîne que la base (OU, OV) est minimale. Supposons que le côté OU soit de longueur minimale. Par conséquent, voir la figure 2, le sommet V appartient à la région délimitée par $\Delta(OU)$ et extérieure à la réunion des cercles de centres O et U et de rayon OU .

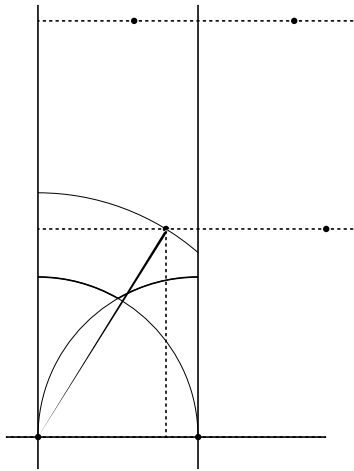


FIG. 2. *

Figure 2. — Un triangle réduit contient la base minimale

Soient v_x et v_y les composantes de OV dans la base orthonormée associée aux directions OU et OU^\perp . La restriction imposée à OV montre que l'on a $v_y/v_x \geq 1$. Il s'en déduit que $3v_y^2 > v_x^2$ et que $4v_y^2 > v_x^2 + v_y^2$ d'où il résulte que $2v_y > \|OV\|$.

Si l'on considère un point quelconque du réseau d'indice de Bézout $\neq \pm 1$ son module est toujours supérieur ou égal à $2v_y$ donc strictement supérieur au module de OV . On voit donc que le vecteur de module minimum OW , parmi les points W du réseau non colinéaires à OU , est atteint sur les pointillés d'indices ± 1 ; c'est le vecteur OV ou le vecteur VU . La base (OU, OV) (ou (OU, VU)) est bien minimale.

Réciproquement, si la base (OU, OV) est minimale il est clair que les 3 côtés OU , OV et UV vérifient la condition (μ) , par conséquent le centre du cercle circonscrit à OUV est intérieur au triangle.

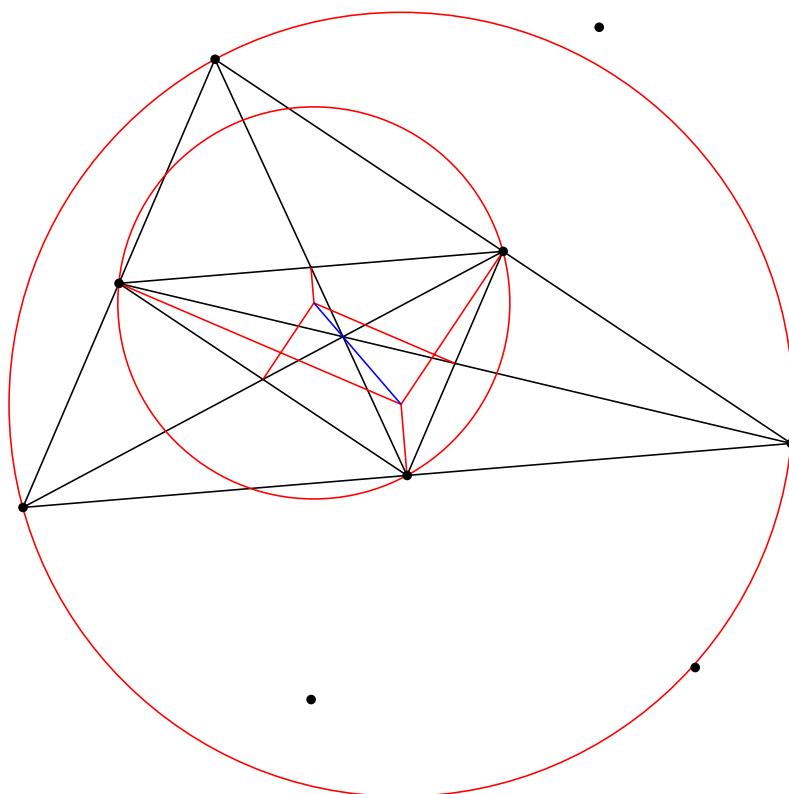


FIG. 3. *

Figure 3. — La droite d'Euler du triangle OAB

Montrons que b) implique c). Cette assertion résulte immédiatement des propriétés de la droite d'Euler du triangle OUV . La figure 3 représente un réseau \mathcal{G} et une base minimale $\{OU, OV\}$; I désigne le centre du cercle circonscrit à OUV , I' est l'orthocentre de ce triangle. Tout résulte du fait que la longueur du segment II' est égale au rayon R du cercle circonscrit ssi OUV est un triangle

rectangle. Si $II' \leq R$ le cercle circonscrit ne peut pas contenir les points de \mathcal{G} tels que O', U', V' , ni les autres. Par contre si $II' > R$ le point O' appartient à ce cercle et le triangle OUV n'est pas Delaunay. Un raisonnement plus synthétique utilisant les propriétés de minimalité bien connues du diagramme de Voronoï d'un ensemble de points, i.e. ceux du réseau, montre que la base minimale forme le triangle fondamental d'une triangulation duale de ce diagramme ; or celle-ci est la triangulation de Delaunay du réseau ; la figure 4 donne un exemple de diagramme de Voronoï d'un réseau entier de rang 2 et de sa triangulation duale de Delaunay.

Réciproquement si un triangle OUV du réseau est Delaunay, comme la triangulation qu'il induit est duale du diagramme de Voronoï associé au réseau, les propriétés de plus proche voisin de ce complexe impliquent que l'une des arêtes du triangle OUV , par exemple OU , atteint la plus courte distance entre deux points du réseau. L'une des arêtes non colinéaire à OU issues de O donne le deuxième vecteur de la base minimale.

Le théorème 1 ci-dessus montre qu'il est utile de savoir déterminer la base minimale d'un sous-groupe \mathcal{G} en partant d'une base quelconque $\mathcal{B} = (OU, OV)$. Il est facile de concevoir un algorithme permettant d'en construire en diminuant le rayon du cercle circonscrit au triangle OUV en rapprochant l'un de ses sommets de la médiatrice du segment opposé.

Supposons que OU soit le plus petit côté du triangle OUV et considérons la parallèle Δ à OU passant par V . Comme O, U, V sont des points entiers, Δ contient une infinité de points de \mathcal{G} de la forme $OV + k.OU$. L'un d'entre eux, noté K est le plus proche de la médiatrice du segment OU ; voir aussi la figure 1 où K était noté V' . On vérifie facilement que le rayon du cercle circonscrit à OUK est inférieur à celui du cercle passant par O, U et V . De plus la base est minimale si $V = V'$.

La décroissance du rayon du cercle circonscrit résulte de l'expression bien connue exprimant cette grandeur en fonction de la longueur des côtés et de l'aire du triangle inscrit. Rappelons que si T est un triangle dont les longueurs des côtés sont α, β, γ et dont l'aire est σ , alors le rayon de son cercle circonscrit est

$$R = \frac{\alpha\beta\gamma}{4\sigma}$$

Il est clair que l'étape de réduction faisant passer de OV à OV' ne change rien si $OV = OV'$ et diminue la longueur d'au moins un des côtés du triangle sinon, celles des deux autres et son aire restant invariantes. Par conséquent, si la base n'est pas minimale, le rayon du cercle circonscrit diminue strictement.

Ceci peut être itéré tant que le centre du cercle circonscrit à OUV est extérieur au triangle. Dès que le centre du cercle circonscrit est à l'intérieur du triangle, le quotient entier $\left[\frac{OU.OV}{|OU|^2} \right]$ est nul quel que soit le couple OU, OV considéré. L'algorithme s'arrête et le triangle obtenu est un triangle de Delaunay du réseau.

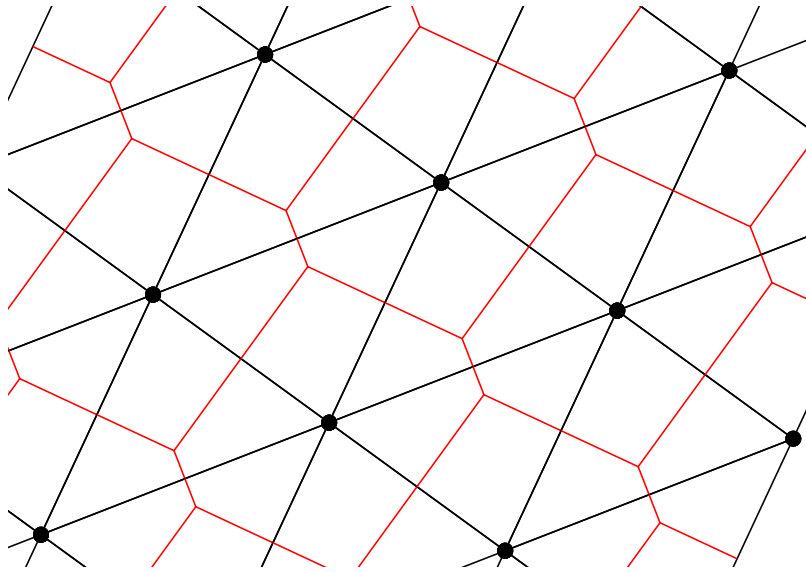


FIG. 4. *

Figure 4. — Diagrammes de Voronoï et de Delaunay d'un réseau

4 – Implémentations Maple des algorithmes de réduction et de plus proche voisin

La procédure **Base**(a, b, c) ci-dessous donne **une** base du sous-groupe \mathcal{G} défini par l'équation diophantienne $ax + by + cz = 0$. L'algorithme est essentiellement celui de Blankinship. La base obtenue est ensuite réduite par l'algorithme de réduction contenu dans la procédure **Red2**.

Pour des raisons de généralité les paramètres a, b, c transmis à la procédure **Base** ne sont pas supposés premiers entre eux, mais on suppose qu'ils vérifient les contraintes $0 < a < b < c$.

```

Base :=proc(a,b,c)
local B,g,M,L,C1,C2,C3,p,x,y :
L :=[a,b,c] :
C1 :=array([a,1,0,0]) :
C2 :=array([b,0,1,0]) :
C3 :=array([c,0,0,1]) :
g :=igcd(op(L)) :
y :=max(op(L)) :
while y<g do
x :=min(op(L)) :
member(x,L,'p') :
if p=1 then
C2 :=evalm(C2-scalarmul(C1,iquo(L[2],L[1]))) :
C3 :=evalm(C3-scalarmul(C1,iquo(L[3],L[1]))) :
elif p=2 then
C1 :=evalm(C1-scalarmul(C2,iquo(L[1],L[2]))) :

```

```

C3 :=evalm(C3-scalarmul(C2, iquo(L[3], L[2])));
else
C1 :=evalm(C1-scalarmul(C3, iquo(L[1], L[3])));
C2 :=evalm(C2-scalarmul(C3, iquo(L[2], L[3])));
fi :
L :=[C1[1], C2[1], C3[1]] :
y :=max(op(L)) :
M :=matrix([evalm(C1), evalm(C2), evalm(C3)]);
M :=transpose(M) :
print(M);
od :
B :=NULL :
if C1[1]=0 then B :=B, convert(C1, list)[2..4] fi :
if C2[1]=0 then B :=B, convert(C2, list)[2..4] fi :
if C3[1]=0 then B :=B, convert(C3, list)[2..4] fi :
[B] :
end :

```

L'algorithme de réduction d'une base d'un sous-groupe de rang 2 de \mathbb{Z}^3 se déduit du critère de minimalité vu au paragraphe 3. La totalité des détails contenus dans la procédure **Red2** ne méritent pas d'être présentés ici; nous nous contentons de donner le cœur de cette procédure dans le cas d'une base $\mathcal{B} = (OU, OV)$, de \mathbb{Z}^2 où $|OU| \leq |OV|$ et $|OU| \leq |OV - OU|$. Dans ce cas l'essentiel de la procédure Maple de réduction à la forme minimale, qui peut être considérée comme une généralisation de l'algorithme de Perron-Frobenius, est donnée ci-dessous.

```

q = [OU.OV / |OU|^2]
tantque q ≥ 1 faire
  OV = OV - qOU
  change(OU, OV)
  q = [OU.OV / |OU|^2]
fin tantque

```

La procédure **Voisin** (B, V) suivante détermine le point du sous-groupe \mathcal{G} engendré par B le plus proche du point V . On suppose ici que \mathcal{G} est de rang 2 dans \mathbb{Z}^3 et que V est un point *rationnel* du plan euclidien contenant \mathcal{G} .

```

Voisin :=proc(B, V)
local nu, P, min, del, x :
nu[1] :=B[1] : nu[2] :=B[2] :
# origine du paralllogramme contenant V :
P :=evalm(scalarmul(nu[1],
floor(evalm(V&*nu[1] / evalm(nu[1]&*nu[1])))
+scalarmul(nu[2],
floor(evalm(V&*nu[2] / evalm(nu[2]&*nu[2]))));
# le sommet du paralllogramme bas en P le plus proche de V.
min :=evalm(evalm(P)&*evalm(P)) :del :=[0, 0, 0] :
x :=evalm(evalm(P-nu[1])&*evalm(P-nu[1])) :
if x<min then min := x : del :=nu[1] fi :
x :=evalm(evalm(P-nu[2])&*evalm(P-nu[2])) :

```

```

if ximin then min := x : del :=nu[2] fi :
x :=evalm(evalm(P-nu[1]-nu[2])&*evalm(P-nu[1]-nu[2])) :
if ximin then min := x : del :=nu[1]+nu[2] fi :
evalm(P+del) :
end :

```

Ces questions étant plutôt délicates nous allons les illustrer avec une application ; soient $a = 3, b = 7, c = 11$, on détermine une base du groupe \mathcal{G} d'équation $3x + 7y + 11z = 0$:

Base(3, 7, 11);

Les calculs intermédiaires donnent deux matrices :

$$\begin{pmatrix} 3 & 1 & 2 \\ 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 7 & -2 & 1 \\ -3 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

et on obtient la base

$$B := \{[7, -3, 0], [1, -2, 1]\}$$

que l'on réduit :

$$B := \mathbf{Red2}([1], [2]);$$

$$B := \{[5, 1, -2], [1, -2, 1]\}.$$

On cherche l'élément de ce groupe le plus proche du point V de coordonnées : $V := [-31/6, -251/14, 141/11]$;

$$\mathbf{Voisin}(B, V);$$

et on obtient le point :

$$[-7, -19, 14].$$

5 – Réseaux entiers, bases, minimalité et Delaunay

On s'intéresse aux réseaux entiers, i.e. aux sous-groupes de \mathbb{Z}^n . On sait trouver, au moyen de l'extension de l'algorithme d'Euclide donnée par Blankinship ([3]), au moins une base d'un tel réseau. Une base du groupe discret \mathcal{G} sera notée $\mathcal{B} = \{b_1, b_2, \dots, b_n\}$. Le déterminant $\Delta = \det(\mathcal{B})$, appelé volume fondamental de la base \mathcal{B} est invariant pour toutes les bases de \mathcal{G} .

Les bases construites algorithmiquement sont généralement très « effilées », (formées de longs vecteurs) ce qui les rend peu exploitables dans les applications concrètes qu'on veut en faire. Or d'après Minkowski, on sait qu'il existe toujours des bases *minimales*, formées de vecteurs les plus courts possibles ; celles-ci simplifient par exemple la recherche du point d'un réseau le plus voisin d'un point donné, qui est l'un des problèmes que nous avons rencontré à plusieurs reprises dans ce texte. On aimerait également réduire les bases par une approche la plus géométrique possible.

Considérons le premier vecteur minimal de \mathcal{G} , soit μ_1 , il est clair que la boule ouverte de \mathbb{Z}^n de centre O et de rayon $\|\mu_1\|$ ne contient pas d'autre

point de \mathcal{G} hormis l'origine O . De même si nous examinons les deux premiers vecteurs minimaux μ_1 et μ_2 , la boule ouverte de même centre, mais dont le rayon est cette fois égal à $\|\mu_2\|$, ne contient pas d'autres points de \mathcal{G} autres que O et $\pm\mu_1$. Par conséquent la sphère (de dimension $n - 1$), circonscrite aux points O, μ_1, μ_2 , (pour alléger nous notons de la même façon l'extrémité d'un vecteur et le vecteur), étant contenue dans la boule précédente, ne contient pas d'autres points de \mathcal{G} . Cette dernière est donc, d'après une définition bien connue en Géométrie Algorithmique, une *sphère de Delaunay* de l'ensemble formé par les points de \mathcal{G} . Le raisonnement se prolonge à toutes les dimensions et montre que les sphères circonscrites aux suites partielles $\mu_1, \mu_2, \dots, \mu_k, k \leq n$, sont Delaunay. Il existe par conséquent une relation étroite entre la recherche des bases minimales et celle de la triangulation de Delaunay d'un réseau, cette dernière étant duale de sa décomposition en cellules de Voronoï ([1]).

A chaque étape de la définition d'une base minimale, les $k - 1$ premiers vecteurs minimaux étant déjà choisis, le minimum des longueurs des vecteurs de \mathcal{G} qui n'appartiennent pas au sous-espace $[\mu_1, \mu_2, \dots, \mu_{k-1}]$ peut être atteint par plusieurs éléments. Par conséquent il n'existe pas en général de base minimale *canonique* dans un réseau entier.

6 – Simplexes et sphères circonscrites

Le rapprochement entre les bases minimales et la condition de Delaunay des sphères circonscrites aux suites partielles $\mu_1, \mu_2, \dots, \mu_k, k \leq n$ d'une telle base suscite une approche plus géométrique de la réduction des bases.

Rappelons que le k -simplexe défini par $k + 1$ points s_0, s_1, \dots, s_k de \mathbb{R}^n , noté $\sigma = \langle s_0, s_1, \dots, s_k \rangle$, désigne leur enveloppe convexe euclidienne.

On désignera par S^{k-1} la sphère de \mathbb{R}^k ensemble des points (x_1, x_2, \dots, x_k) tels que

$$x_1^2 + x_2^2 + \dots + x_k^2 = 1$$

Si \mathcal{F} est une partie compacte de \mathbb{R}^k , finie ou infinie, on désigne par $S^{k-1}(\mathcal{F})$ la sphère de dimension $k - 1$ de plus petit rayon contenant \mathcal{F} . On dit que c'est la sphère englobante de \mathcal{F} . On désigne par $R(S^{k-1})$ le rayon de la sphère S^{k-1} .

Lorsque \mathcal{F} se réduit à un k -simplexe de \mathbb{R}^k , (ou à un ensemble de $k + 1$ points de cet espace), $S^k(\mathcal{F})$ coïncide avec la sphère circonscrite à \mathcal{F} , qui est bien définie.

Un cas important est celui où \mathcal{F} est la réunion d'une sphère de dimension $k - 1$, S^{k-1} et d'un point M de \mathbb{R}^n , où $k \leq n$. Il est bien connu que dans ce cas la sphère englobante $S^k(\mathcal{F})$ est également circonscrite et que son centre se trouve sur l'axe de symétrie (δ) de S^{k-1} qui est orthogonal à l'hyperplan (\mathcal{P}) qu'elle définit. Observer que $S^k(\mathcal{F})$ est également la sphère englobante de la réunion de M et de la sphère $S^k(S^{k-1})$. Cette dernière a une dimension de plus que S^{k-1} mais le même rayon.

Supposons la droite (δ) orientée et désignons par d la distance de M à celle-ci et par h la distance de M à l'hyperplan (\mathcal{P}); on note ρ le rayon de S^{k-1} . Le couple (h, d) constitue les coordonnées cylindriques du point M . Un calcul facile donne l'abscisse (algébrique) du centre de la sphère circonscrite à \mathcal{F} sur la droite (δ).

Si 0 et ω représentent respectivement les centres des sphères S^{k-1} et $S^k(\mathcal{F})$, on a

$$\overline{0\omega} = \frac{h^2 + d^2 - \rho^2}{2h}$$

Autrement dit, lorsque $h > 0$, on a $\overline{0\omega} > 0$ si M est extérieur à la sphère S^{k-1} et $\overline{0\omega} \leq 0$ sinon. (1)

Un résultat analogue est vrai lorsque $h < 0$. On en déduit la valeur du rayon $R(S^k(\mathcal{F}))$, noté R dans la suite.

$$R^2 = \rho^2 + \frac{(h^2 + d^2 - \rho^2)^2}{4h^2}$$

On désigne par S^{k-1} une sphère de dimension $k-1$ comme ci-dessus et par \mathcal{E}^+ l'ensemble des points de \mathbb{R}^n pour lesquels $h > 0$. Si $M, M' \in \mathcal{E}^+$ on note \mathcal{F} , (resp. \mathcal{F}') les compacts $\{S^{k-1} \cup M\}$, (resp. $= \{S^{k-1} \cup M'\}$).

Dans ces conditions la valeur du rayon de la sphère circonscrite à $\mathcal{F} = \{S^{k-1} \cup M\}$ induit un ordre sur les points M de \mathcal{E}^+ .

On notera $M \prec M'$ si M est intérieur à la sphère $S^k(\mathcal{F}')$ et $M \preceq M'$ si M est intérieur ou appartient à la sphère $S^k(\mathcal{F}')$.

Il est bien sûr équivalent de dire que l'on a $M \prec M'$ si $R(S^k(\mathcal{F})) < R(S^k(\mathcal{F}'))$ et que $M \preceq M'$ si $R(S^k(\mathcal{F})) \leq R(S^k(\mathcal{F}'))$. (2)

7 - Classification géométrique des simplexes

Considérons un k -simplexe $\sigma = \langle s_0, s_1, \dots, s_k \rangle$ et sa sphère circonscrite S^{k-1} ; soit s_{k+1} un point de \mathcal{E}^+ . On désigne par σ le $k+1$ -simplexe $\langle s_0, s_1, \dots, s_{k+1} \rangle$ et par S^k la sphère circonscrite à ce dernier de centre ω et de rayon R . Rappelons qu'un même simplexe, par exemple σ , possède des sphères circonscrites de dimensions distinctes, par exemple $S^{k-1}(\sigma)$ et $S^k(\sigma)$; ces dernières ont le même centre ω et le même rayon R mais des dimensions $k-1$ et k différentes.

On dit qu'un simplexe est *bien étoilé* ssi il contient le centre de sa sphère circonscrite. Un simplexe qui ne vérifie pas cette propriété est dit *mal étoilé*.

On a le résultat suivant.

Lemme 1. — *Un $k+1$ -simplexe $\sigma = \langle s_0, s_1, \dots, s_{k+1} \rangle$ est bien étoilé ssi tout sommet s_i est extérieur à la k -sphère circonscrite à sa face opposée $\langle s_0, s_1, \dots, \hat{s}_i, \dots, s_{k+1} \rangle$ (où $\hat{}$ signifie l'omission).*

Démonstration. Un simplexe est bien étoilé ssi aucune face ne sépare le sommet opposé et le centre de la sphère circonscrite. La i -ème face $\langle s_0, s_1, \dots, \hat{s}_i, \dots, s_k \rangle$ de σ étant désignée par f_i on note 0_i le centre de sa sphère circonscrite (de dimension $k-2$ ou k) et, comme auparavant ω désigne le centre de la sphère circonscrite à σ . Les axes (δ_i) associés aux faces f_i sont orientés positivement lorsqu'ils *entrent* dans le k -simplexe σ , Soient (h_i, d_i) les coordonnées cylindriques du sommet s_i relativement à sa face opposée f_i , comme ci-dessus. Avec ces notations la condition σ *bien étoilé* équivaut à dire que pour tout i la composante $0_i\omega$ du centre ω sur l'axe (δ_i) est positive.

D'après la propriété (1) des sphères circonscrites vue au § précédent ceci équivaut à dire que pour tout i le sommet s_i est extérieur à la sphère de dimension $k - 1$ circonscrite à la face f_i de dimension $k - 1$.

On vérifie facilement qu'un simplexe est mal étoilé ssi il existe une face séparant ω du sommet opposé; on dira que c'est la *face séparante* du simplexe mal étoilé (il n'en existe qu'une seule).

Considérons un simplexe non dégénéré bien étoilé et soit R le rayon de sa sphère circonscrite; alors le rayon de la sphère circonscrite d'une de ses faces est inférieur ou égal à R . En effet une sphère circonscrite est aussi une sphère englobante, i.e. de plus petit rayon...

Pour un simplexe mal étoilé dont la face séparante est f , le rayon de la sphère circonscrite à celle-ci est supérieur aux rayons des sphères circonscrites aux autres faces.

La condition (2) du paragraphe précédent implique que si l'on remplace un sommet d'un simplexe par un point intérieur à sa sphère circonscrite, le rayon de sa sphère circonscrite diminue.

Le résultat suivant est évident.

Lemme 2. — *Les rayons des faces d'un simplexe sont tous majorés par le rayon de sa sphère circonscrite.*

Il a une conséquence intéressante.

Corollaire 1. — *Soit σ un k -simplexe diamétral d'une sphère S^k de rayon ρ et M un point quelconque de S^k , alors les rayons des faces du simplexe $M * \sigma$ (joint de M et σ) sont tous inférieurs à ρ . Le résultat est encore vrai si M est intérieur à S^k .*

8 – Algorithme de réduction d'une base

Soit \mathcal{G} un sous-groupe de rang n de \mathbb{Z}^n et $\mathcal{B} = \{u_1, \dots, u_n\}$ une de ses bases dont la forme volume vaut Δ ; on désigne par Σ le n -simplexe $\langle s_0, s_1, \dots, s_n \rangle$ associé à cette base; $s_0 = O$ et pour $i \geq 1$ s_i est l'extrémité de μ_i . Si \mathcal{H} désigne le sous-groupe de \mathcal{G} engendré par les $n - 1$ premiers vecteurs u_1, \dots, u_{n-1} , soit ν le vecteur directeur de la droite (euclidienne) orthogonale à \mathcal{H} défini par $u_1 \wedge u_2 \wedge \dots \wedge u_{n-1}$. Le sommet s_n est l'une des solutions de l'équation diophantienne

$$\nu.X = \Delta$$

où X est un vecteur entier quelconque $X = (x_1, x_2, \dots, x_n)$.

Réduire la base \mathcal{B} de \mathcal{G} consiste, intuitivement, à trouver d'autres solutions de cette équation diophantienne ainsi que des équations analogues associées aux autres faces, de sorte que le simplexe associé soit le plus *petit* possible; ce qui est le cas si le simplexe est bien étoilé. Ces réductions ont été illustrées plus haut au §3.

Supposons que le n -simplexe de rayon R associé à une base de \mathcal{G} soit mal étoilé. On peut le réduire *modulo* sa face de rayon minimal, ceci donne un nouveau n -simplexe dont le rayon de la sphère circonscrite est strictement inférieur à R . Ce dernier est soit bien étoilé, soit mal étoilé.

Théorème 3. — *Si la réduction d'un n -simplexe mal étoilé Σ modulo la face f_i est un nouveau simplexe mal étoilé Σ' , alors f_i est la face séparante du simplexe Σ' .*

Démonstration. Soit Σ le n -simplexe de rayon R associé à la base de \mathcal{G} et σ la face de plus petit rayon et S^{n-1} la sphère associée à ce $n - 1$ -simplexe σ . Ce dernier est diamétral pour S^{n-1} . Soit s le sommet de Σ opposé à σ et \mathcal{H} le sous-groupe affine de \mathcal{G} translaté du sous-groupe associé à σ passant par s . On note (\mathcal{P}) le plan euclidien associé à ce sous-groupe affine.

Réduire la base revient à remplacer s par le point de \mathcal{H} le plus proche du centre de la sphère S^{n-1} , soit μ .

Si le point μ est extérieur à S^{n-1} alors le nouveau n -simplexe est bien étoilé et l'algorithme s'arrête. Si μ est à l'intérieur de S^{n-1} alors le nouveau simplexe Σ est mal étoilé (ne pas oublier que σ est diamétral) et toutes ses faces (hormis σ) ont un rayon inférieur à ρ ; σ est bien la nouvelle face séparante. Il suffit de chercher la nouvelle face de rayon minimum.

Autrement dit soit on obtient un simplexe bien étoilé (et on s'arrête), soit on obtient un simplexe mal étoilé, mais alors les rayons des faces (et du simplexe) diminuent strictement. Pour un simplexe bien étoilé on ne peut pas aller plus loin, la base est *réduite* et nous conjecturons qu'elle est minimale.

9 – Conclusion

L'extension du champ d'application de l'informatique nécessite une utilisation croissante de notions et résultats théoriques provenant de presque tous les domaines mathématiques. Même les *discrétisations* générales qui ont souvent été perçues comme des opérations hautement destructrices peuvent tirer bénéfice, si elles sont bien définies, les secteurs auxquels elles sont naturellement apparentés tels que l'algèbre et l'arithmétique. De nombreux travaux actuellement poursuivis dans ce sens contribueront certainement à améliorer l'image que certains secteurs appliqués ont encore trop souvent dans la communauté mathématique.

Bibliographie

- [1] BOISSONNAT (J.-D.) ET YVINEC (M.) .— *Géométrie algorithmique*. — Ediscience international, 1995.
- [2] BRESENHAM (J.). — *Algorithm for computer control of a digital plotter*. IBM System Journal, 1965, vol. 4, pp. 25-30.
- [3] BLANKINSHIP W.A. — *A new version of the Euclidean algorithm*. Amer. Math. monthly, pp. 742-745, 1963.
- [4] COHEN (D.) ET KAUFMAN (A.E.). — *Fundamentals of surface voxelisation*, CVGIP-GMIP, 57 (6), No. 95, pp. 453-461.
- [5] I. DEBLED-RENNESON. — *Etude et reconnaissance des droites et plans discrets*. — Thèse, Université Louis Pasteur, Strasbourg, France, déc. 1995.
- [6] DEBLED (I.) ET REVEILLÈS (J.-P.) — *A New Approach to Digital Planes*. — Vision Geometry III, (R.A. Melter, A.Y. Wu eds.), Boston 1994, pp. 12-21, SPIE vol. 2356.
- [7] DEBLED (I.) ET REVEILLÈS (J.-P.) — *A linear algorithm for the segmentation of discrete curves*. — In Parallel Image Analysis and applications. Series in

- Machine Perception artificial intelligence, Vol. 19 pp. 73-100, World Scientific 1996, ISBN 981-02-2476-1
- [8] ERDÖS (P.), GRUBER (P.M.) ET HAMMER (J.). — Lattice points. Longman Scientific & Technical. 1989.
 - [9] HARDY (G.H.) ET WRIGHT (E.M.) — An introduction to the theory of number, fifth edition, Oxford Sc. Pub., 1989.
 - [10] KAUFMAN (A.E.). — *Volume synthesis*. 6th International Workshop, Discrete Geometry for Computer Imagery 96, Lyon, France, November 1996. Lecture Notes in Computer Science, Springer Verlag.
 - [11] KONG (T.I.) ET ROSENFELD (A.) . — *Digital Topology : Introduction and survey* — Computer Vision, Graphics and Image Processing 48, pp. 352-393, 1989.
 - [12] LANG (S.) . — Algebra, 3rd edition. Addison-Wesley. 1994.
 - [13] LENSTRA (A. K.), LENSTRA JR. (H.W.) ET LOVÁSZ (L.) . — *Factoring polynomials with rational coefficients*, Math. Ann. 261 (4) pp. 515-534, 1982.
 - [14] REVEILLÈS (J.-P.). — *Géométrie discrète, calcul en nombres entiers et algorithmique*, —Thèse d'État, Strasbourg, 1991.
 - [15] REVEILLÈS J.-P. ET YAACOUB (J.). — *MAT Operator for contour extraction*. *Journal of Electronic Imaging*,
 - [16] ROSENFELD (A.). — Picture processing by computer, Acad. press, N.-Y. 1969.
 - [17] ROSENFELD (A.). — Picture Languages, Acad. press, N.-Y. 1979.
 - [18] ROSENFELD (A.). — *Digital straight lines segments*, I.E.E.E. Trans. on Computers, t. **23**, 12, 1974, p. 1264-1369.
 - [19] SEROUL (R.). — Informatique pour mathématiciens. Masson 1996.

Un résumé des travaux de T. Gowers

Gilles GODEFROY (*Université Paris 6*)

Les travaux les plus importants de T. Gowers concernent la géométrie des espaces de Banach (voir [G1]) et l'analyse combinatoire finie (voir [G2]).

Les espaces de Banach ont été initialement conçus pour appliquer des idées topologiques (comme le théorème de Baire) ou géométriques (comme le théorème de Hahn-Banach) à des problèmes concrets d'analyse fonctionnelle, avant d'être étudiés pour eux-mêmes. La simplicité de leur définition recèle une grande complexité, dès lors qu'on sort du cadre topologique très simple dans lequel ils sont d'ordinaire utilisés. Ainsi, une classification des espaces de Banach à isomorphisme près paraît totalement hors de portée. Cependant, la théorie contient des résultats généraux et importants dont la démonstration est très délicate, ainsi que des exemples très élaborés. La contribution de T. Gowers dans ces deux directions est fondamentale.

William Timothy Gowers

Parmi les espaces de Banach, les espaces réticulés (c'est-à-dire essentiellement ceux qui sont isomorphes à des espaces ordonnés de fonctions ou de suites) ont une structure simple et bien comprise. Il est donc naturel de se demander si tout espace est de ce type ou du moins contient un sous-espace de ce type. Cette question a été résolue négativement en 1991 indépendamment et simultanément par T. Gowers et B. Maurey. Leur exemple d'espace de Banach sans suite basique inconditionnelle, dont la norme est définie inductivement (et apparaît donc comme un point fixe d'une certaine fonctionnelle), s'est révélé jouir de propriétés « négatives » très fortes : ainsi, aucun de ses sous-espaces fermés ne peut s'écrire comme somme directe de deux sous-espaces fermés de dimension infinie ; en d'autres termes, l'espace est *héréditairement indécomposable* (H.I.). Une modification de la construction a permis à T. Gowers de résoudre aussitôt après une question remontant à S. Banach, en montrant l'existence d'un espace de dimension infinie non isomorphe à ses hyperplans (ni à aucun sous-espace strict) avant de montrer avec B. Maurey qu'un opérateur sur un espace H.I. est toujours somme d'un opérateur scalaire et d'un opérateur strictement singulier, ce qui montre qu'en fait tout espace H.I. fournit une réponse négative à la question de S. Banach.

La structure d'un espace X a ainsi d'importantes conséquences sur celle de l'algèbre $L(X)$ des opérateurs continus de X dans X . Dans certains cas, une réciproque peut s'établir : par exemple, un théorème montré en 1971 par J. Lindenstrauss et L. Tzafriri énonce que tout espace de Banach dont tout sous-espace fermé est l'image d'une projection continue est isomorphe à l'espace de Hilbert. Un espace qui a « beaucoup » de projections est donc Hilbertisable. T. Gowers a montré en 1993 qu'on pouvait remplacer « projection » par « isomorphisme » dans le théorème ci-dessus : il établit en effet qu'un espace de Banach isomorphe à tous ses sous-espaces de dimension infinie est isomorphe à l'espace de Hilbert. Cette solution du problème de l'« espace homogène » repose d'une part sur un théorème de R. Komorowski et N. Tomczak-Jaegermann affirmant que tout espace de cotype fini contient l'espace de Hilbert ou un sous-espace sans base inconditionnelle et d'autre part sur le *théorème de dichotomie* de Gowers : tout espace de Banach contient un sous-espace H.I. ou un sous-espace à base inconditionnelle. En d'autres termes, tout espace de Banach contient soit un « très bon », soit un « très mauvais » sous-espace. Ce résultat fondamental repose sur un théorème combinatoire encore plus général obtenu par une utilisation subtile des jeux topologiques et dont les applications ne sont certainement pas épuisées. Notons au passage que le théorème de l'espace homogène s'ensuit du théorème de dichotomie, sans qu'il soit nécessaire d'établir l'*existence* d'un espace H.I. D'autres résultats importants ont été montrés par T. Gowers en géométrie des espaces de Banach : parmi ceux-ci, la construction d'un espace ne contenant ni sous-espace isomorphe à l_1 , ni sous-espace à dual séparable, ainsi que l'existence d'un espace isomorphe à son cube mais pas à son carré, qui montre en particulier que deux espaces de Banach non isomorphes peuvent être tels que chacun d'entre eux est isomorphe à un sous-espace complémenté de l'autre espace. Il est clair que ses travaux ont approfondi et complètement renouvelé toute la théorie.

Le point de départ des travaux de Tim Gowers en combinatoire finie est le célèbre théorème de Szemerédi, qui énonce que pour tout entier $k > 0$ et tout réel $\delta > 0$, il existe un entier N tel que tout sous-ensemble de $\{1, 2, \dots, N\}$ de cardinal au moins $\delta \cdot N$ contient une progression arithmétique de longueur k . La démonstration du cas général, obtenu par Szemerédi en 1975, est de nature combinatoire et les bornes obtenues par sa méthode pour l'entier N , fonction de k et de δ , sont si grandes qu'il faut utiliser une notation spéciale pour les énoncer ; elles nécessitent au moins le sixième niveau de la hiérarchie de Ackermann. Le cas particulier $k = 3$ avait cependant été obtenu dès 1953 par K. Roth par une méthode de sommes d'exponentielles donnant dans ce cas de bien meilleures estimations, de l'ordre d'une exponentielle trois fois itérée de l'inverse de la densité δ , estimation ensuite améliorée par Heath-Brown et Szemerédi. Un approfondissement de la méthode de Roth a permis à T. Gowers d'établir le cas $k = 4$ du théorème de Szemerédi, avec N de l'ordre d'une exponentielle deux fois itérée d'une puissance négative de la densité. Tim Gowers est très probablement en possession du cas général et donc d'une amélioration quantitative extrêmement forte du théorème de Szemerédi, mais selon ses termes, il souhaite attendre que la difficile démonstration pour k quelconque soit vérifiée avant d'affirmer le résultat. La méthode de Gowers dans le cas

$k = 4$ utilise donc des sommes d'exponentielles et plus précisément l'analyse de Fourier sur les groupes cycliques. La stratégie consiste à établir une dichotomie sur les sous-ensembles dans lesquels on veut construire des progressions arithmétiques : ils sont « uniformes » ou « concentrés ». Le premier cas correspond à la petitesse de la transformée de Fourier de leur fonction caractéristique ; cette idée de Roth est ici modifiée et Gowers considère et utilise des ensembles « quadratiquement uniformes ». Le second cas intervient quand l'un des coefficients de Fourier est grand. Gowers montre alors l'existence d'une progression arithmétique sur laquelle la trace de l'ensemble a une densité plus grande, ce qui permet un argument itératif. L'un des outils essentiels de cette partie est une modification d'un théorème de Freiman qui montre quantitativement que les ensembles A d'entiers tels que $A + A$ ne soit pas beaucoup plus grand que A sont contenus dans des sommes de progressions arithmétiques. Notons que le théorème de van der Waerden, qui énonce que pour tout couple d'entiers (k, l) , il existe $N = N(k, l)$ tel que pour toute partition de $\{1, 2, \dots, N\}$ en k sous-ensembles, l'un de ces sous-ensembles contient une progression arithmétique de longueur l , est une conséquence immédiate du théorème de Szemerédi. Les travaux de Gowers améliorent considérablement les bornes extrêmement grandes connues jusqu'à présent pour le théorème de van der Waerden. Remarquons enfin que les méthodes de Tim Gowers sont par certains aspects proches de techniques classiques en théorie des nombres. Elles pourraient s'interpréter comme un progrès vers la construction de grandes progressions arithmétiques dans des ensembles naturels, comme l'ensemble des nombres premiers.

Bibliographie

- [G1] W. T. GOWERS, *Recent results in the theory of infinite-dimensional Banach spaces*, Proceedings of the International Congress of Mathematicians, Zürich (1994), 933-942.
- [G2] W. T. GOWERS, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, *Geom. and Funct. Anal.* vol 8 (1998), 529-551.